

Standard Operating Procedure

System Security Plan Numbering Schema

ITS-SOP-0007B

Version Date: 20080401

Effective Date: 20080417

Expiration Date: 20110417

Responsible Office: Office of the Chief Information Officer

Document Change and Review History

| Version Number | Summary of Changes | Changes Made/Reviewed By | Date |
|----------------|---|--------------------------|---------|
| 1.0 | Updated to reflect the ITSC four-digit numbering schema for master plans and added a master system field for non-NASA (external) systems. Also added several functional office codes. | S. Adair | 7/19/07 |
| 1.1 | Edit for grammar, style and structure | K. Collins | 8/28/07 |
| 1.2 | Final updates for delivery back to S. Adair | A. Darling | 8/30/07 |
| 1.3 | Remove ITSC and master/subordinate references | A. Keim/D. Kniffin | 3/26/08 |
| 1.4 | Edit for structure and formatting | T. Fryer | 4/1/08 |

TABLE OF CONTENTS

| | |
|--|----------|
| 1. PURPOSE | 1 |
| 2. SCOPE | 1 |
| 3. APPLICABLE DOCUMENTS | 1 |
| 4. ROLES AND RESPONSIBILITIES | 1 |
| 5. PROCESS | 1 |
| 6. APPROVAL | 4 |
| APPENDIX A: GLOSSARY..... | 5 |

1. Purpose

This SOP establishes NASA's standard numbering schema for identifying Information Technology (IT) system security plans. The schema retains the existing System Security Plan Registry numbering, and links the unique identifier to the responsible Authorizing Official (AO) and the responsible Center.

2. Scope

This SOP applies to all personnel involved in the IT security of NASA information systems.

3. Applicable Documents

The following documents were used to update this SOP:

- a. ITS-SOP-0007A

4. Roles and Responsibilities

The following roles and responsibilities are applicable to this SOP:

Information System Owner (ISO)

- a. Assigns all portions of the security plan numbering schema and uses this SOP as guidance to ensure the applicable fields are assigned appropriately.

Security Documentation Creator/Preparer

- a. Ensures that the security plan numbering schema fields are entered into the IT Security documentation repository appropriately and updated as necessary.

5. Process

5.1 Security Plan Numbering Schema

All IT system security plans shall have a unique identifier that consists of multiple fields separated by hyphens.

- AA-mmm-a-bbb-nnnn

An explanation of each field follows.

- a. [AA]

This is a two letter field that identifies the functional office that is responsible for the system security plan. There are currently 21 possible functional offices and sub-offices with Authorizing Officials that can accredit NASA information systems. Accordingly, this field must have one of the following values:

AR Aeronautics Research Mission Directorate

CD Multi-Program systems which support multiple Mission Directorates (authorized by the Center Deputy Director or Center CIO)

| | |
|----|---|
| ED | Chief Education Officer |
| EG | Office of the Chief Engineer |
| ER | External Relations |
| EX | Exploration Systems Mission Directorate |
| FO | Office of the Chief Financial Officer |
| GC | Office of General Counsel |
| HM | Office of Chief Health and Medical Officer |
| IE | Integrated Enterprise Management Program |
| IG | Office of Inspector General |
| IM | Institutions and Management Mission Support Directorate |
| IO | Office of Chief Information Officer |
| IP | Innovative Partnership Program |
| OA | Office Automation Information Technology (OCIO) |
| OS | Office of Security and Program Protection |
| PA | Office of Program Analysis and Evaluation |
| PI | Program and Institutional Integration |
| SC | Science Mission Directorate |
| SO | Space Operations Mission Directorate |
| SP | Office of Safety and Mission Assurance Systems |

In the case of an external system that contains NASA information, in compliance with ITS-SOP-0033, this field shall contain the following two-letter code:

| | |
|----|-----------------------------|
| NN | External (Non-NASA) Systems |
|----|-----------------------------|

b. [mmm]

This is a three digit numeric field that can be used to identify the system within a Center. If a Center chooses not to utilize this field for internal organizational identification, this number can default to '999'.

c. [a]

This is a single letter field that identifies the FIPS-199 security categorization of the system:

L – Indicates the system is Low

M – Indicates the system is Moderate

H – Indicates the system is High

d. [bbb]

This is a three letter field that identifies the Center that is responsible for tracking the system. This is usually where the system is located, managed, or reported. There are 12 possible values for this field, as follows:

| | |
|-----|-------------------------------|
| ARC | Ames Research Center |
| DFR | Dryden Flight Research Center |
| GRC | Glenn Research Center |
| GSF | Goddard Space Flight Center |
| JPL | the Jet Propulsion Laboratory |
| JSC | Johnson Space Center |
| KSC | Kennedy Space Center |
| LRC | Langley Research Center |
| MSF | Marshall Space Flight Center |
| NHQ | NASA Headquarters |
| NSS | NASA Shared Services Center |
| SSC | Stennis Space Center |

e. [nnnn]

This is a four digit numeric field that identifies the system. This number is unique within all of NASA and provides historical tracking of a system. It never changes, even if other parts of the identifier change.

Examples:

The following examples are provided:

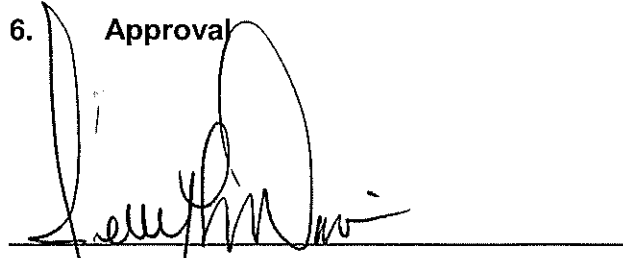
OA-101-L-DFR-1002

This is an example of a valid system security plan number for an OAIT LAN System located at the Dryden Flight Research Center.

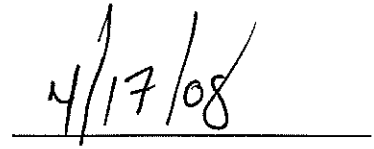
SO-999-L-KSC-6601

This is an example of a valid system security plan number for a Space Operations system located at Kennedy Space Center.

6. **Approval**

A handwritten signature in black ink, appearing to read "Jerry L. Davis", is written over a horizontal line.

Jerry L. Davis
Deputy CIO IT Security
Senior Agency Information Security Officer

A handwritten date "4/17/08" is written in black ink over a horizontal line.

Date

Appendix A: Glossary

| Acronym | Term | Explanation |
|---------|--------------------------|--|
| AO | Authorizing Official | A NASA official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals. |
| ISO | Information System Owner | An agency official responsible for overall procurement, development, integration, modification, or operation and maintenance of an information system. Responsible for the development and maintenance of the security documentation and ensures the system is deployed and operated according to the security requirements. |
| IT | Information Technology | Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. |